GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

National Cyber Security Centre

Cyber Threat Report

2017/18

New Zealand Government

Contents

Foreword

The National Cyber Security Centre, part of the Government Communications Security Bureau, helps protect New Zealand's organisations of national significance from advanced cyber threats and responds to cyber incidents that have a high impact on New Zealand. This report aims to provide insight into the types of cyber threats and incidents encountered by these organisations.

The National Cyber Security Centre's activity relies on the consent and cooperation of our customers and the New Zealand public. For this reason, it is important that we build and maintain trust in all we do. This year Project CORTEX, the NCSC's advanced cyber security initiative, received the 2018 Institute of Public Administration New Zealand (IPANZ) Award for "Building Trust and Confidence in Government", as well as "New Zealand's Best Security Project or Initiative" at the 2018 Information Security Awards New Zealand (iSANZ). This reflects the hard work undertaken by NCSC staff to successfully deliver cyber security services to our nationally significant customers.

Since the completion of Project CORTEX, the NCSC has continued working to improve its advanced cyber network defence capabilities. The Malware Free Networks initiative was piloted successfully in 2017 and received Cabinet endorsement for wider rollout. This capability will allow us to work with a greater number of organisations of national significance, and their internet service providers, to disrupt malicious cyber activity.

This year the NCSC also released the first Cyber Security Resilience report[1], which benchmarks the cyber security resilience of New Zealand's nationally significant organisations. The report summarises survey data collated from 250 nationally significant organisations; and identifies that, despite an increased investment in cyber security in the past 12 months, organisations feel their security practices are not keeping pace with the rate of digital transformation. The report also identifies four key areas (governance, investment, readiness and supply chain) where organisations could focus to improve themselves, and provides practical steps to assist this.

In the reporting year from 1 July 2017 to 30 June 2018, the NCSC recorded 347 cyber security incidents, with a 'cost avoidance' benefit to nationally significant organisations in the order of NZD$27m. Due to the NCSC's focus, this is only a subset of the total incidents affecting New Zealand.[2] This year, 134 incidents (39 percent of the total) contained elements that had been linked to known state-sponsored cyber actors. Additionally, the vast majority of incidents were detected at, or prior to, an actor's first attempt to compromise an organisation, minimising the harm experienced by New Zealand organisations.

This year has seen a shift in the cyber threat landscape, with changes in technology and adversary tactics influencing the types of cyber activity seen. We have observed continued targeting of New Zealand for espionage and revenue-generation purposes; while globally, foreign nations have increased their disinformation and political interference activity, which has resulted in western nations responding with public condemnations of such malicious activity. The NCSC and its partners will continue to denounce cyber activity that threatens the safety and security of cyberspace.

We hope this report will promote informed discussion about cyber security practices and contribute to the increased resilience of New Zealand's information systems and the security and wellbeing of New Zealanders.

Lisa Fong
Director, National Cyber Security Centre

1 This report can be found at: https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Cyber-Security-Resilience-Assessment-F-WEB.pdf

2 https://www.cert.govt.nz/about/quarterly-report/

By the numbers

347

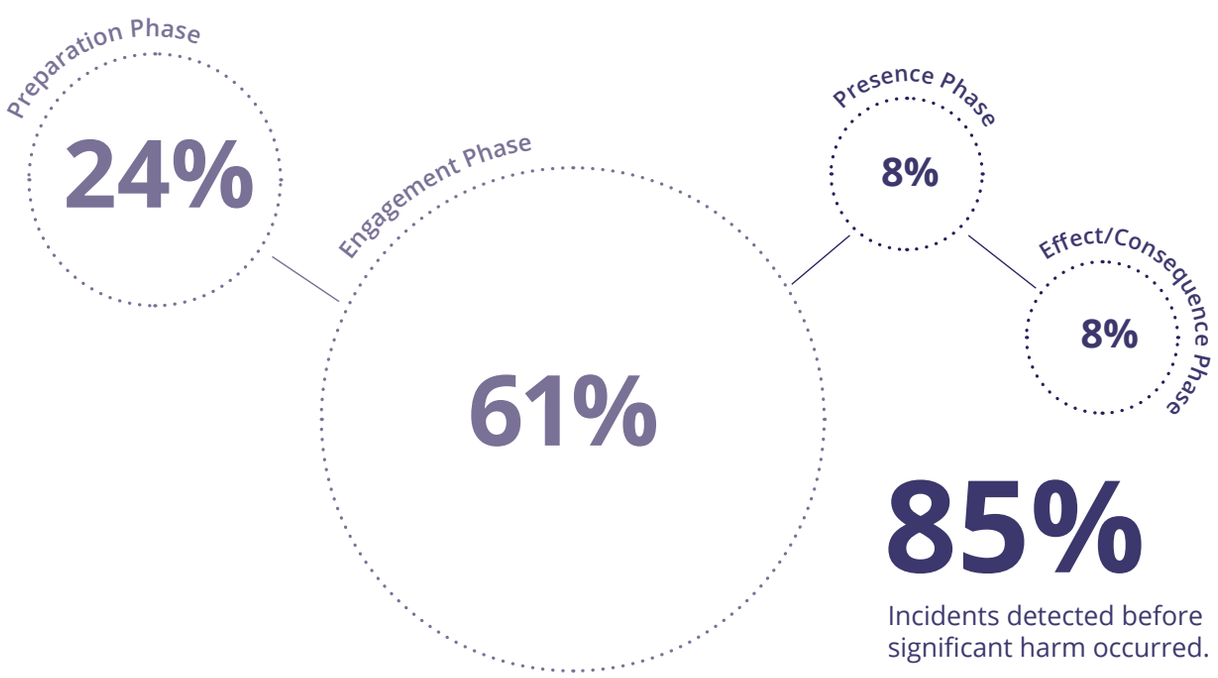
Total recorded cyber incidents.

396 in 2016/17

39%

Incidents linked to state sponsored actors.

33% in 2016/17



85%

Incidents detected before significant harm occurred.

$26.9million

Worth of harm reduced through operation of GCSB cyber threat defence capabilities.

~$67m since June 2016

About the National Cyber Security Centre

The National Cyber Security Centre (NCSC) is part of the Government Communications Security Bureau. Our role is to protect New Zealand's most significant public and private sector organisations from high impact, advanced cyber threats, and to ensure the security and integrity of New Zealand's communication and information infrastructures.

What we do

The NCSC provides detection and disruption services, specialist security information and advice, as well as incident response capabilities to nationally significant organisations. These organisations include government departments, key economic generators, research institutes and operators of critical national infrastructure. Additionally, we engage more broadly with organisations representing key industry groups. The NCSC coordinates a number of regional and sector-based security information exchanges where information security professionals can confidentially share information; and we share threat prevention and mitigation advice with our customers and partners.

Cyber defence

The NCSC works to protect New Zealand from cyber threats that could impact our national security or economy.

In July 2017 the NCSC completed Project CORTEX which delivered a suite of advanced cyber defence capabilities and services to our customers. The NCSC continues to improve and advance these capabilities, and as such has been developing the Malware Free Networks initiative in 2018. This work involves the NCSC working with internet service providers to deliver 'active disruption' of cyber threats.

Following a successful pilot programme, Cabinet approved the continued development and implementation of Malware Free Networks, which was announced in May 2018. Planning for the scalability and implementation of the project began shortly after.

Who we work with

In order to effectively protect New Zealand and New Zealanders from advanced cyber threats, the NCSC works closely with a range of domestic and international agencies.

The NCSC, CERT NZ (New Zealand's Computer Emergency Response Team) and New Zealand Police work to ensure the New Zealand Government's response to cyber events is effective and comprehensive. New Zealand Police is responsible for responding to crimes occurring online and CERT NZ works to support businesses, organisations and individuals who are affected by cyber security incidents. The NCSC responds to cyber incidents involving organisations of national significance or where the security and/or economic prosperity of New Zealand may be impacted. In the case of a severe or critical cyber incident, the NCSC would also work with the Department of Prime Minister and Cabinet, Department of Internal Affairs, and the Ministry of Foreign Affairs and Trade to provide a whole of government response to the incident.

Internationally, the NCSC works closely with the Australian Cyber Security Centre; the United Kingdom's National Cyber Security Centre; the Canadian Centre for Cyber Security; the United States of America's (US) National Security Agency and the worldwide CERT community to better understand the international cyber threat environment and provide greater protection to New Zealand entities.

Did you know?

The New Zealand Government is committed to increasing the use of Te Reo Māori, one of New Zealand's official languages. Here are a few basic terms you can learn and use, along with their English translation.

Whakahaumaru – *security*

Wheinga – *adversary, opponent*

Mūrere – *to hack, hacker*

Pūkaha pāpori – *social engineering*

Hitinihanga – *phishing*

The global cyber threat landscape

Digital transformation continues to evolve internationally, with ever more devices connected to the internet, and organisations increasingly reliant on technology for everyday activities.

Malicious cyber actors, including both state-sponsored and criminal actors, continue to target computer systems for an ever increasing range of reasons, utilising the continually evolving range of technologies and tools at their disposal.

This rate of technological change results in an increasingly complex cyber threat environment, both in New Zealand and internationally; where everyone - individuals, organisations and nations must be conscious about cyber security.

The international threat landscape has seen an increased use of cyber operations to advance nation states' goals, such as the disinformation or influence campaigns intended to disrupt other nations' political systems, like that seen in the 2016 US presidential election. Large-scale public breaches of personal information have promoted the issue of data privacy amongst the public consciousness, and developing technologies continue to increase the attack surface available to cyber actors.

Increased attack surfaces

The risks posed to supply chains and managed service providers (MSPs) continue to grow as organisations increasingly outsource parts of their business to third parties. The highly interconnected nature of these supply chain systems mean cyber actors no longer need to directly target the customer organisation if the third party is more easily compromised. Why break in the front door when your neighbour's front door is open and they have a key to your house?

Attack surface

The attack surface simply means the sum of all points where an actor can try to enter a system, or where they can extract data from. A network with many data interfaces has more vulnerabilities (or potential attack surfaces) to exploit, than a network with a few carefully controlled access points.

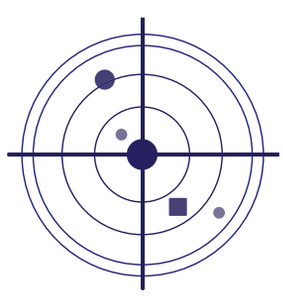
Supply chain

Supply chain means all suppliers that contribute to the content of a product or system, or have the opportunity to modify the content.

Managed service providers

A managed service provider is an information technology services provider that manages and assumes responsibility for providing a defined set of services to its clients. Services can include IT system management, data backup, cloud storage and network security.

Organisations making use of MSP services for network defence need to ensure their MSP is fulfilling its IT security responsibilities.

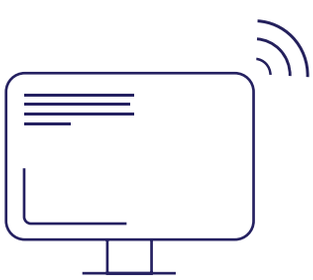


Internet of Things (IoT)

The IoT is the collective term used for physical devices that are fitted with sensors or software enabling them to be accessed, controlled and monitored remotely. These devices range from household items (heat pumps/light bulbs), to medical devices (pacemakers), and components integral to the operation of critical national infrastructure (power grids/hydroelectric dams/nuclear reactors).

Another area that will increasingly impact organisations and individuals is the 'Internet of Things'. Many of these devices are not being designed with security in mind, and there will often be no way to patch or upgrade software when security vulnerabilities are identified. Organisations should be aware of the risks that come with IoT, and demand 'security by design' from vendors. Further, individuals should be aware of the personal data these devices collect (such as physical location, work times and habits), making IoT devices an attractive target for cyber actors.

As more 'things' are connected to the Internet, the importance of, and consumer reliance on, the underlying network will grow. The next generation of mobile communication technology, 5G, promises to provide more data, to more customers, faster, with much lower latency levels. To do this, 5G networks will place data closer to the end user, using virtualisation technologies rather than having core functions centralised in one location. The spread of these 'core' functions across the network increases the attack surface, making it more difficult to protect the confidentiality, availability, and integrity of the data traversing the network.



Privacy of data

Recent instances of data breaches and corporate misuse of customer data have elevated online privacy concerns into public discourse. This has led to an increase in consumer awareness of their online privacy rights and as such, lawmakers have been shaping legislation to hold organisations accountable for poor network security. For example, the European Union's (EU) General Data Protection Regulation legislation came into effect in May 2018 and applies to all organisations that have customers, or hold data on, individuals residing in the EU. In the case of a data breach, organisations have particular obligations they must undertake, or risk facing a heavy fine.

Changing cyber operations

This year has seen a rise in the use of cyber operations that test the threshold of acceptable activity in cyberspace, and advance non-traditional goals for nation state groups. This activity has included states undertaking financial cyber operations to monetise criminal activity; the use of destructive ransomware such as BadRabbit, which rendered IT inoperable and created chaos across Russia and Ukraine; attacks on highly public events such as the 2018 Winter Olympics, which serve no financial or espionage goals; and subversive influence campaigns intended to disrupt or influence other nations' political systems, such as the compromises of the US Democratic National Committee or the German Bundestag.

These types of activity serve no national security interest, are occurring with more frequency, and have resulted in significant damage and disruptions to computer systems, public services and organisations. These events also impact the safety and autonomy of people online.

By publically condemning these activities, New Zealand and its international partners hope to both deter such activity in future, and send a signal indicating acceptable behaviour standards in cyberspace. For example, New Zealand and other nations have released statements condemning the NotPetya and WannaCry attacks from 2017, linking the Russian Government to four malicious cyber campaigns since 2015, and attributing the compromise of global managed service providers in 2016 to a group affiliated with the Chinese Government. Where necessary, New Zealand will continue to do this in future.

The New Zealand landscape

Traditionally, New Zealand has been isolated from many security threats due to its geographic remoteness. However, given the interconnected nature of the internet, cyber threats can travel thousands of kilometres to impact New Zealanders directly.

With the growth of internet society, New Zealand is now closely connected to the global digital economy. New Zealand's internationally-focused and market-driven economy has taken advantage of this integration, and New Zealanders have benefited greatly from the ease and availability of information, goods and services. New Zealanders have become increasingly reliant on the internet not only for trade and business, but also social interactions and entertainment. In the eyes of malicious cyber actors, this increasing connectivity and adoption of digital services increases the available attack surface and potential accessibility of New Zealand information infrastructures and networks.

New Zealand individuals, businesses and government agencies can be targeted by cyber actors looking to exploit any poor security practices or vulnerabilities in networks, so everyone must be conscious of, and alert to, cyber risks.

New Zealand entities face both direct and indirect cyber threats

Direct threats have a specific and deliberate target that they are tailored to exploit. A New Zealand entity can be targeted for the purpose of extracting New Zealand-specific information, such as cyber espionage aimed at government departments, or the theft of intellectual property from a New Zealand company.

Indirect threats on the other hand are more indiscriminate, and delivered widely, in the hopes of compromising any vulnerable individual or organisation. While indirect threats are largely untargeted, they will still have a theme, for example targeting English-speaking nations, or users of a particular technology. Indirect threats are typically less sophisticated, but can still cause harm to New Zealand.

NCSC recorded incidents

The NCSC becomes aware of incidents from a number of sources, including detection by NCSC's advanced cyber defence capabilities, self-reporting by the victim, and reporting from our domestic and international partners.

During the 2017/18 period, the NCSC recorded and responded to 347 cyber security incidents.

In 29 cases this year, the NCSC identified potential vulnerabilities in customer networks that, although not being actively targeted by cyber actors at the time, still posed a risk. In response, the NCSC proactively notified relevant customers of the vulnerability and recommended mitigations. In addition, the NCSC provided 155 reports to customers, alerting them to potential cyber security incidents or risks. In high priority incidents, the NCSC provides hands-on intensive incident response; and did so on 22 occasions in the past year.

Not all incidents are created equal. Detecting and removing an unopened phishing email is recorded as one incident by the NCSC, as is the compromise of an entire network along with the exfiltration of organisational data. These two examples have significantly different impacts on the organisation involved, and require vastly different amounts of effort to resolve, yet each is counted as one incident.

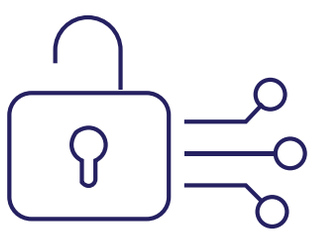
Therefore the number of incidents recorded in a year does not necessarily reflect the state of the cyber threat environment, or the amount of work required by the NCSC to respond. This is why the NCSC records the types and phase of detected activity to identify more thematic changes in the tactics and behaviour of cyber actors. Further details on this are provided in the cyber threat framework section (Figure 1).

This financial year has seen continued changes in technology and adversary techniques and tradecraft. As the NCSC is attempting to raise the cyber security maturity of New Zealand organisations, actors themselves are becoming more mature and making use of new technologies as they become available. Additionally, some state-sponsored cyber actors have taken to more covert and discriminate operations, while others have overtly targeted non-traditional targets, such as media outlets or politicians.

This year the NCSC has focused on detecting incidents at an earlier stage in the lifecycle, when the impact – both in terms of cost and harm to the organisation – is reduced, as well as focusing on the threats from more sophisticated actors.

What is a cyber incident?

The NCSC defines a cyber security incident as 'an occurrence or activity that appears to have degraded the confidentiality, integrity or availability of data within an information infrastructure'.



The impact of the NCSC's work

In 2016, the NCSC commissioned independent research to help quantify the economic benefits of our Project CORTEX's advanced cyber threat detection and disruption capabilities and services. This research established the approximate cost avoided by NCSC's cyber defence capabilities.

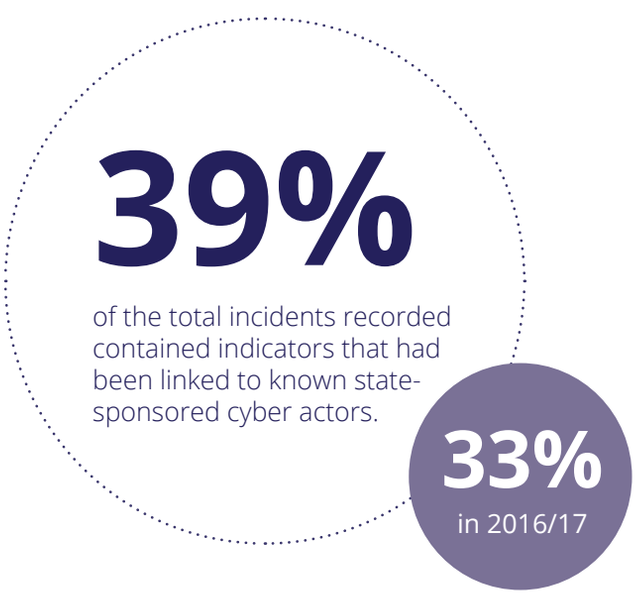
This 'cost avoidance' model was applied again for the 2017/18 period and assessed the threats detected or mitigated through the operation of NCSC's capabilities resulted in a conservatively estimated "gross reduced harm benefit" of $27m to New Zealand. This means, in the two years since July 2016, Project CORTEX has reduced an approximate total of NZD$67m in harm to New Zealand organisations.

Who did it?

Given the global, borderless nature of the online environment, and the ability of cyber actors to utilise tools and infrastructure from across numerous countries, it is very difficult to assign specific responsibility for an act to an individual. The process of attribution can be expensive, and will depend on the resources available to the agency. The NCSC has the advantage of close relationships with international partners to assist in this.

Attribution is most commonly used to help assess the intent of an actor, or the potential impact of an incident. The most frequent form of attribution undertaken by NCSC is when an incident is detected through, or discovered to contain, indicators or technical artefacts that have previously been associated with state-sponsored activity. In the past year, 134 incidents (39 percent of the total incidents recorded) contained indicators that had been linked to known state-sponsored cyber actors.

This is both a numerical and proportionate increase from the previous reporting period, indicating the increasing ability of the NCSC to detect and counter cyber threats from sophisticated actors, to protect New Zealand's networks of national importance.



Case studies

Privacy

In one instance impacting the privacy and freedom of an individual in New Zealand, the NCSC assisted a foreign national, who had recently claimed asylum in New Zealand. The individual had previous political connections and had campaigned for pro-democracy movements in their home country. The NCSC identified that individual's computer had been infected with malware associated with a state-sponsored group, which provided the adversary the ability to record all keystrokes, remotely monitor the victim's screen and copy files without detection. In this instance, the NCSC attributed the compromise to a foreign intelligence service. The NCSC worked with the individual to remediate the infection and provide security advice to reduce the risk of further compromises.

Outdated software

In early 2018, using the CORTEX platform, the NCSC detected crypto-currency mining malware on a large number of computers within a customer network. The malware had been installed by criminal actors who intended to generate revenue by using the affected organisation's computing power and resources for their own operations. Analysis by the NCSC identified the actors had installed the malware through a vulnerability in outdated remote access software that was managed by the customer's IT provider. The NCSC worked with the customer and their IT provider to ensure the malware was removed and the outdated software was updated.

Network security

The security of network devices continues to be a target for state-sponsored groups. This year the NCSC identified poor security practices related to a network device commonly used by a large number of New Zealand organisations. A feature of the device, which was designed to be used internally, when exposed to the internet presents a risk of unauthorised access that could potentially be used as an entry point into an organisation's wider network. The NCSC notified affected organisations of the risk they were carrying, and released a public advisory for awareness of the issues associated with exposing these devices to the internet.

Cyber threat framework

The wide variety of tools and techniques available to cyber actors and criminals makes it difficult to produce a precise taxonomy of cyber intrusions, but a network compromise is not a singular event. It occurs in a series of stages, each of which provides the NCSC an opportunity to detect, mitigate or block adversary activity.

What is it?

The cyber threat framework provides a scalable, actor-agnostic methodology that can be used to chart the typical life cycle of a compromise. Lifecycle analysis, with slight variation, is used widely in the cyber security industry and by the NCSC and its partners.[3]

The phases can be split into activities that occur prior to the initial compromise, and those that occur after;

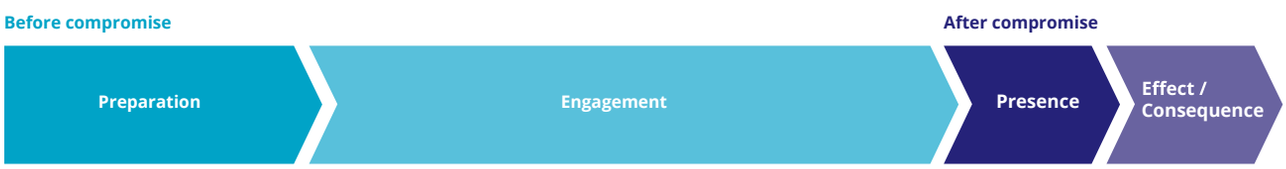


Figure 1

Preparation Phase

In the preparation phase, the actor would begin by identifying potential targets, and through research and reconnaissance begin to understand the target's weaknesses. It is here the actor would gather the necessary resources and begin to allocate the infrastructure and capabilities required for the operation. Actors may select targets, conduct scanning, or develop infections for phishing emails or websites. It is often very difficult to clearly identify malicious activity in this phase.

Engagement Phase

The engagement phase is the first 'active' step taken by the actor, with the intent to gain initial access. In this phase, a malicious payload is delivered to the target through exploiting vulnerabilities in technology, people or processes, and the exploitation of this payload subsequently provides the actor unauthorised access to the target's system. One of the most common methods of payload delivery is phishing emails.

Presence Phase

The goal of the presence phase is to ensure ongoing and robust access to the target's system. This may be achieved through internal reconnaissance of the network, lateral movement to compromise additional systems, or detection avoidance measures. Establishing persistence on the target's network may involve escalating user privileges for a compromised account, or installing and hiding tools that enable backdoor access.

Effect/Consequence Phase

In the effect/consequence phase, the actor likely achieves their mission objective which may involve the exfiltration, degradation, or disruption of data or infrastructure. At this stage it is very difficult and expensive to remove an actor from one's systems.

For a cyber actor to achieve their goal in the effect/consequence phase, they would first typically undertake some form of activity in each of the previous phases. If this activity can be detected and mitigated in an earlier phase, the overall impact on the organisation can be reduced.

3 The NCSC mostly draws on the Common Cyber Threat Framework – available online at www.dni.gov/index.php/cyber-threat-framework

The cyber threat framework enables the NCSC to categorise and analyse incidents, to determine the sophistication of the threat and the potential impact on an organisation. In doing so, the NCSC is able to determine the appropriate level of response required to ensure the vulnerabilities of, or damage to, an organisation's networks are mitigated effectively.

As illustrated by Figure 1, almost 85 percent of this year's categorisable incidents were detected at, or prior to, the cyber actor's first probe of an organisation.[4] These initial attempts at compromise were generally not successful, limiting the potential damage to New Zealand organisations by malicious cyber actors. The earlier an incident is detected in the lifecycle, the faster it can be remediated, and usually with less disruption and cost to the organisation.

How we use it

This framework helps the NCSC identify weaker areas in the security of New Zealand organisations, as well as determine trends in malicious cyber activity. For example, of the incidents that reached a post-compromise phase, the most common methods of compromise were malware installation and exploiting network device vulnerabilities. In comparison, the incidents that reached the same phases last year involved the compromise of websites and data breaches which are more readily detected.

In addition, of the 134 incidents that have been linked to state-sponsored cyber actors, only 12 reached the presence or effect/consequences phase, the majority of which involved compromised routers being used to access an organisation. This indicates the NCSC is detecting and mitigating the majority of state-sponsored threats before they are able to cause harm to New Zealand organisations.

The simple things still work

This year saw the continued use of simple, but effective, attack tools.

Phishing emails continue to be a very popular delivery mechanism for cyber actors because they target the weakest link in an organisation's network security – the human. Phishing emails are often used to deliver malware, which frequently requires some form of user interaction to download onto a device. In combination, malware and phishing emails account for nearly one third of all categorised incidents this past year.

Phishing emails can also be used to deliver credential harvesting links, or falsified business invoices.

Credential harvesting is the practice of convincing users to enter their legitimate login details into a spoofed website controlled by the actor. This enables the actor to use these credentials to avoid detection. This is a growing risk for organisations due to the number of online or cloud services that are accessed using credentials.

Falsified business invoices can involve the transfer of large sums of money to an actor. This can be achieved through the actor pretending to be an organisation executive and requesting an invoice be paid. Simple checks of bank account or email address details can help mitigate these often expensive mistakes. In three incidents reported to the NCSC this year, New Zealand organisations lost nearly NZD$800,000 to 'successful' fraudulent invoice emails.

4 NB. Approximately 25 percent of incidents this year could not be categorised into a phase, as they involved the NCSC proactively notifying organisations of potential vulnerabilities (therefore addressing the issue prior to any actor activity), false positive results, or lacked adequate information for categorisation. These incidents have not been included in the graph.

Conclusion

The global and domestic cyber threat environment is constantly changing, keeping pace with the rate of change in technology and tools. In order to continue defending New Zealand's economic and national security, the NCSC must keep pace with these changes too.

New Zealand and the world are becoming ever more reliant on the internet in all aspects of life. This increasing uptake of digital services and devices creates more and more targetable connections every day; while the ability to purchase exploitation tools enables actors with a lower level of technical skill to have a disproportionately negative impact. As such, New Zealanders are becoming increasingly vulnerable to malicious cyber activity.

This year has seen a rise in nation states utilising cyber operations to test the threshold for acceptable activity in cyberspace. Nations have conducted cyber operations to monetise criminal activity, attack public events like the 2018 Winter Olympics, and influence campaigns to impact political systems such as the US 2016 presidential election.

Activities like these challenge the international rules-based order of cyberspace, which impacts the safety and autonomy of all individuals and organisations online. In response to these activities, New Zealand and its international partners adopted a new proactive approach of publically condemning foreign governments for malicious cyber activity where it threatened the rules of cyberspace.

Public attribution is a way to reduce the efficacy of malicious cyber actors by revealing their tools or increasing the reputational costs of illegitimate activity; however individuals and organisations also need to take steps to protect themselves.

The proliferation of internet-connected devices may be currently designed for an individual's private life, but these will inevitably impact how organisations run their business in the future. Prioritising security and preparing for this future is vital for both organisations and consumers of technology.

The NCSC will continue to work with nationally significant organisations and partners across the public and private sector, to ensure the continued protection of our networks from advanced cyber threats.

Getting in touch with us

If you have any questions related to this report, please contact the communications team at the GCSB.

If you have encountered a cyber incident, please visit our website for further information: **www.ncsc.govt.nz**

Glossary

Below is a glossary of terms that are included to assist readers' understanding. It should not be interpreted as a comprehensive list of terms used by the NCSC to describe the cyber threat environment.

5G Networks	The fifth generation of mobile communications technology that aims to increase the speed, capacity and quantity of data transfer across wireless networks.
Advanced Cyber Threat	A well-resourced, highly skilled cyber actor or group that has the time, resources and operational capability for long-term intrusion campaigns. Their goal is typically to covertly compromise a target, and they will persist until they are successful. They are very capable of compromising secured networks using both publicly disclosed, as well as self-discovered, vulnerabilities.
Backdoor	A feature or defect of a computer that allows unauthorised access to a device or the data stored on it.
Credentials	A user's authentication information used to verify identity – typically a password, token or certificate.
Computer Network Defence	A set of processes and measures to protect devices, services and networks – and the information on them – from theft or damage.
Cyberspace	The global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place.
Cyber Threat	An attempt to undermine or compromise the function of a computer-based system, access information, or attempt to track the online movements of individuals without their permission.
Exfiltration	Where an actor has unauthorised access to private organisational data (for example legitimate credentials, or intellectual property), and removes it from a system, typically in the form of files, database dump or system memory dump.
Incident	An occurrence or activity that appears to have degraded the confidentiality, integrity or availability of a system or network.
Malicious Cyber Actor	An individual or group of people who seek to exploit computer systems to steal, destroy or degrade an organisation's information. Actors may be individual computer hackers, part of an organised criminal group, or state sponsored.
Malware	Malicious software or code intended to have an adverse impact on organisations' or individuals' data, e.g. viruses, Trojans or worms.
Mitigation	Steps that organisations and individuals can take to minimise and address cyber security risks.
Router	A network device which sends data packets from one network to another based on the destination IP address.

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

New Zealand Government